LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

NAMA : FAIZ MAHRDIKA
NIM : 105841113923
KELAS : 5JKA – ETHICAL HACKING

---

1. PENDAHULUAN

Pada era digital saat ini, keamanan informasi merupakan komponen yang sangat penting dalam menjaga keberlangsungan layanan berbasis teknologi, terutama pada institusi pendidikan tinggi seperti **Universitas Negeri Makassar (UNM)**. Sebagai perguruan tinggi negeri yang memanfaatkan berbagai layanan digital—mulai dari sistem informasi akademik, website resmi, layanan administrasi online, hingga portal mahasiswa—UNM memiliki kewajiban untuk memastikan bahwa seluruh sistem tersebut terlindungi dari potensi ancaman dan serangan siber.

Salah satu langkah awal dalam proses pengujian keamanan (penetration testing) adalah tahap **reconnaissance**, yaitu proses pengumpulan informasi sebanyak mungkin mengenai target sebelum dilakukan pengujian lebih lanjut. Tahap ini membantu penyerang maupun penguji keamanan untuk memahami struktur sistem, teknologi yang digunakan, serta potensi kelemahan yang dapat dieksploitasi.

2. RUANG LINGKUP & SKENARIO PENGUJIAN a. Peran dan Tujuan

- **Peran** : Mendukung proses hardening sistem.
- **Tujuan** : Mengumpulkan informasi awal mengenai sistem yang digunakan oleh UNM

b. Target Pengujian

Tabel 1.1 Ruang Lingkup dan Target Pengujian

Fase	**Target yang Diaudit**
Passive Reconnaissance	Website Universitas Negeri Makassar *(unm.ac.id)*
Active Reconnaissance	VM Lab Rentan – IP: **192.168.77.2**

c. Rules of Engagement

Semua aktivitas pemindaian **aktif** hanya dilakukan pada mesin lab dengan IP **192.168.77.2** Pada website publik, hanya dilakukan **pengintaian pasif** tanpa interaksi langsung yang berbahaya.

3. TOOLS & LINGKUNGAN PENGUJIAN

Tabel 1.2 Spesifikasi Alat (Tools) dan Fungsinya

Tools	**Fungsi**
Kali Linux	Sistem operasi pengujian keamanan
Netdiscover	Host discovery jaringan
Nmap	Port, service, dan OS scanning
Wireshark	Analisis protokol jaringan
crt.sh	Pemetaan domain & certificate transparency
BuiltWith	Identifikasi teknologi website
GitHub Search	Pencarian informasi sensitif dan kode publik

Lingkungan pengujian dilakukan pada jaringan lokal untuk memastikan legalitas.

4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan sebagai berikut:

a. Passive Reconnaissance
   - Mengumpulkan data melalui OSINT (Open Source Intelligence)
   - Tidak berinteraksi langsung dengan server

b. Active Reconnaissance
   - Memindai IP target untuk menemukan port dan service terbuka • Mengidentifikasi OS dan protokol jaringan

5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

Target: wakab.go.id

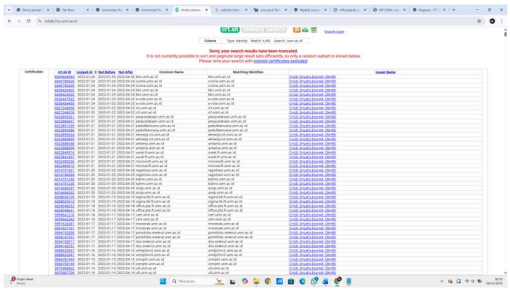
Tabel 1.3 Hasil Pengumpulan Informasi passive reconnaissance

Kategori Informasi	Informasi yang Ditemukan	(Alat/Website)	Alasan Relevansi
Pencarian Sub-domain	kkn.unm.ac.id ict.unm.ac.id icome.unm.ac.id my.unm.ac.id badanpenerbit.unm.ac.id	crt.sh https://crt.sh/?q=unm.ac.id	Menunjukkan permukaan serangan (attack surface) yang lebih luas.
Informasi Karyawan	Kasdy Kadir, S.Pd., M.Pd. (Teknisi Laboratorium) Gunawan Pribadi Yunus (Teknisi Perlatan Kantor) Kartini Kadir, A.Md.Kom. (Pengolah Data)	Website Resmi Pegawai Ft Unm https://ft.unm.ac.id/profil/fasilitas/	Untuk memahami struktur organisasi dan pihak yang relevan.
Format Email	humas@unm.ac.id	info@unm.ac.id	Digunakan untuk validasi pola email dalam simulasi keamanan.
Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith https://builtwith.com/unm.ac.id	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.

Informasi Sensitif Terpapar	Repository GitHub: dystianen/gowakab	GitHub Search (OSINT)	Potensi kebocoran source code atau kredensial.

a. Bukti Dokumentasi

1. Pencarian Domain dan Sub-domain



Gambar 1.1 Hasil Pencarian Subdomain menggunakan crt.sh

Menampilkan daftar subdomain yang terdaftar pada sertifikat SSL, memperluas attack surface.

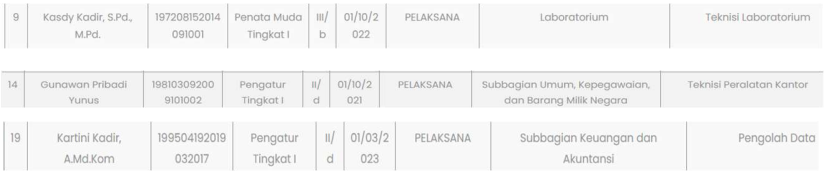
2. Informasi email dan karyawan

- Informasi email

Gambar 1.2 Identifikasi Kontak Publik pada Footer Website

Penemuan alamat email generik (humas@unm.ac.id) yang memvalidasi format domain email organisasi.

- Karyawan FT Unm

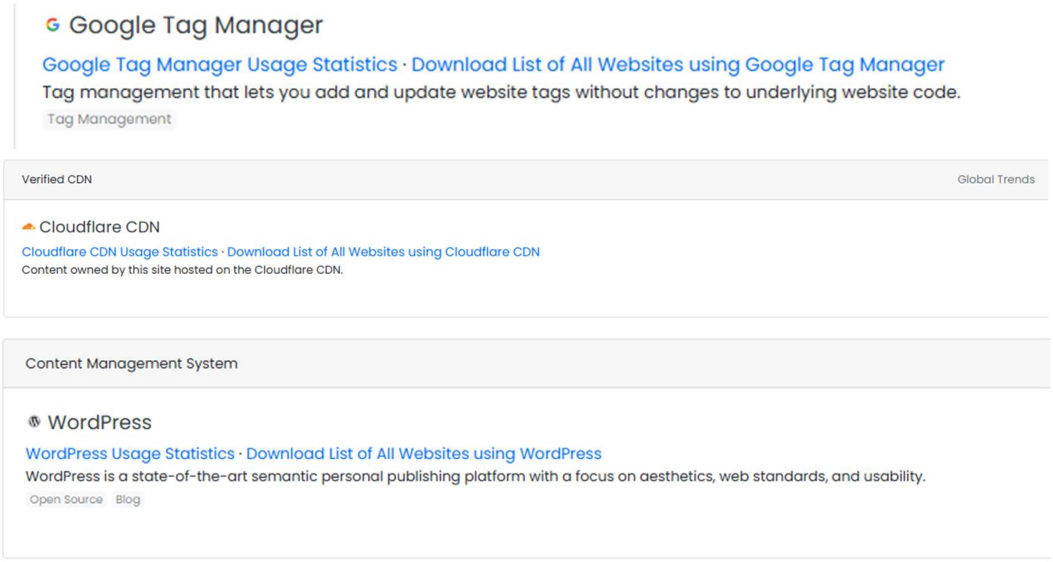


9	Kasdy Kadir, S.Pd., M.Pd.	197208152014091001	Penata Muda Tingkat I	III/b	01/10/2022	PELAKSANA	Laboratorium	Teknisi Laboratorium
14	Gunawan Pribadi Yunus	198103092009101002	Pengatur Tingkat I	II/d	01/10/2021	PELAKSANA	Subbagian Umum, Kepegawaian, dan Barang Milik Negara	Teknisi Peralatan Kantor
19	Kartini Kadir, A.Md.Kom	199504192019032017	Pengatur Tingkat I	II/d	01/03/2023	PELAKSANA	Subbagian Keuangan dan Akuntansi	Pengolah Data

Gambar 1.3 Identifikasi Profil Karyawan Struktural FT Unm

Pengumpulan data personel kunci (High-Value Targets) melalui halaman profil publik untuk pemetaan struktur organisasi.

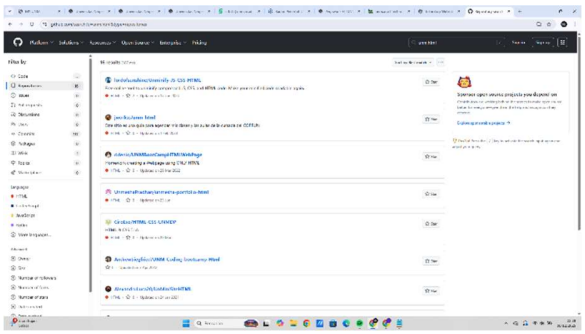
3. Teknologi yang digunakan



Gambar 1.4 Identifikasi Teknologi Website dan Struktur Organisasi Deteksi penggunaan Cloudflare dan daftar karyawan terkait yang rentan terhadap serangan Social Engineering.

Penggunaan Cloudflare menunjukkan bahwa server asli (Origin IP) mungkin tersembunyi di balik WAF (Web Application Firewall). Serangan langsung ke domain utama mungkin akan diblokir, sehingga penyerang kemungkinan akan mengalihkan fokus ke subdomain yang tidak terlindungi Cloudflare (seperti yang ditemukan di crt.sh)

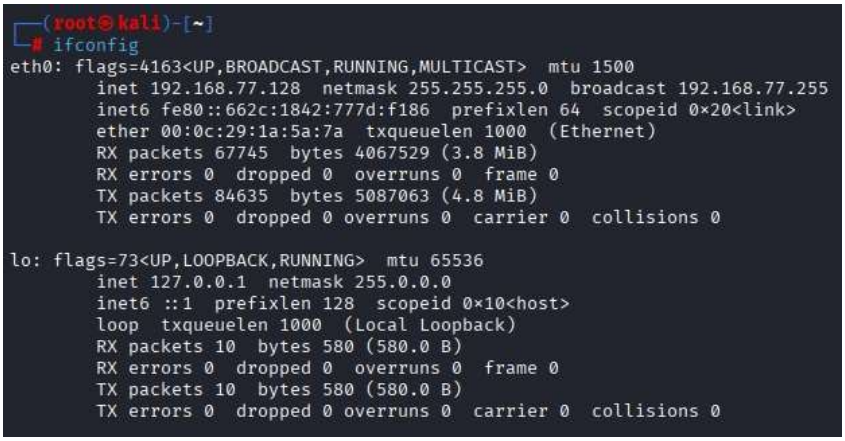
4. Informasi sensitive yang terpapar



Gambar 1.5 Temuan Repository GitHub (OSINT)

Potensi kebocoran source code atau kredensial pada repository publik. Temuan repository pada GitHub (dystianen/gowakab) sangat kritis. Jika pengembang lupa menghapus file konfigurasi (seperti .env atau config.php), penyerang dapat menemukan *hardcoded credentials* (username/password database) yang memungkinkan pengambilalihan sistem tanpa perlu mengeksploitasi celah software

4. ACTIVE RECONNAISSANCE (HASIL & ANALISIS) ifconfig



Gambar 1.6 Konfigurasi IP Attacker (Kali Linux)

Sebelum melakukan pemindaian aktif, verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ifconfig, di mana interface eth0 teridentifikasi memiliki alamat IP 192.168.77.128 dengan netmask 255.255.255.0 (Gambar [Nomor]). Konfigurasi ini mengonfirmasi bahwa penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target192.168.77.255, memvalidasi skenario Internal Network Attack melalui konektivitas Layer 2 (Data Link) yang memungkinkan efektivitas teknik ARP Scanning serta memastikan paket probe Nmap dapat mencapai target tanpa terhalang oleh Network Firewall atau router eksternal."

a. Host Discovery dan Port Scanning

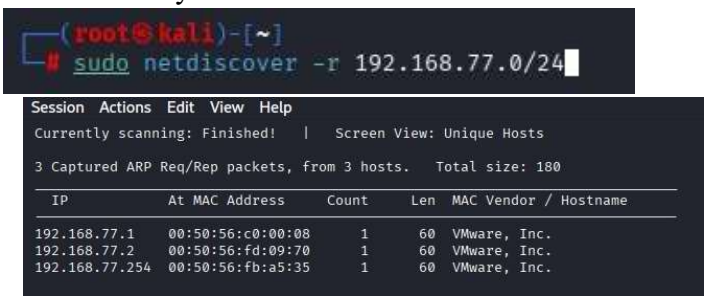
Tabel 1.4 Hasil Pemindaian Host dan Port (Active Reconnaissance

Tugas	Command	Hasil	Potensi Dampak
Host Discovery	sudo netdiscover -r 192.168.77.0/24	Target ditemukan: 192.168.77.255	Memastikan host aktif di jaringan.

TCP SYN Scan	sudo nmap -sS 192.168.77.255	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --topports 20 192.168.77.255	Open/Filtered: 53, 67	DNS dan DHCP berpotensi menjadi target analisis.

a. Dokumentasi

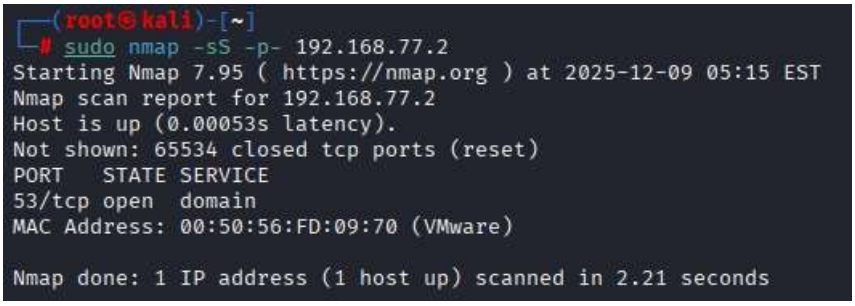
- Host discovery



Gambar 1.7 Hasil Host Discovery dengan Netdiscover

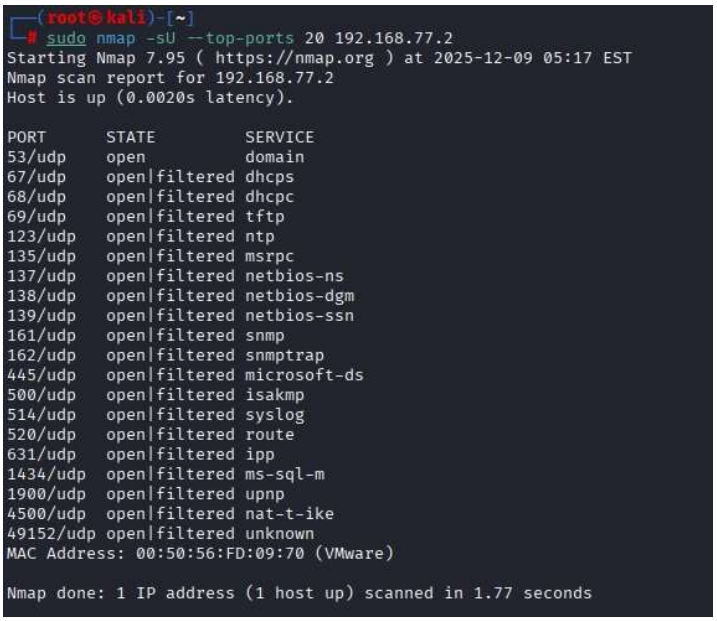
Mengidentifikasi host yang aktif. Target 192.168.77.0/24teridentifikasi menggunakan vendor VMware (volunsOS)

- TCP SYN scan



Gambar 1.8 Hasil TCP SYN Scan (Stealth Scan) Menemukan port TCP terbuka (22, 80, 6667) tanpa menyelesaikan 3-way handshake

- UDP scn



Gambar 1.9 Hasil UDP Scan

Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered

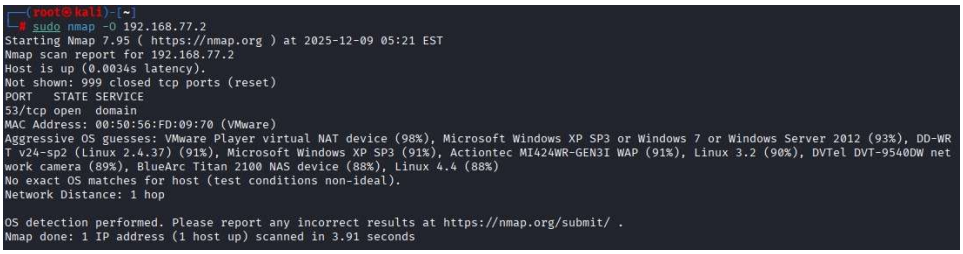
b. Service and Version Detection sudo nmap -sV **192.168.77.0/24**

Tabel 1.5 Deteksi Versi Layanan dan Analisis Kerentanan

Port	Service	Version	Analisis Risiko
22	SSH	OpenSSH 6.6.1p1	Versi lama → potensi brute force & enumeration.
80	HTTP	Apache 2.4.7	Banyak CVE publik untuk versi lama.

6667	IRC	Ngircd	Ditemukannya Port 6667 (IRC) dengan service ngircd adalah anomali besar untuk server pemerintah atau perusahaan. Port ini sering dikaitkan dengan *backdoor* (seperti kerentanan pada UnrealIRCd) atau digunakan oleh botnet untuk Command & Control (C2). Ini adalah prioritas utama untuk tahap eksploitasi selanjutnya

• Bukti service detection



Gambar 1.10 Deteksi Versi Layanan dan Sistem Operasi

Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan OpenSSH 6.6.1p1 dan Apache 2.4.7.

c. OS Fingerprinting sudo

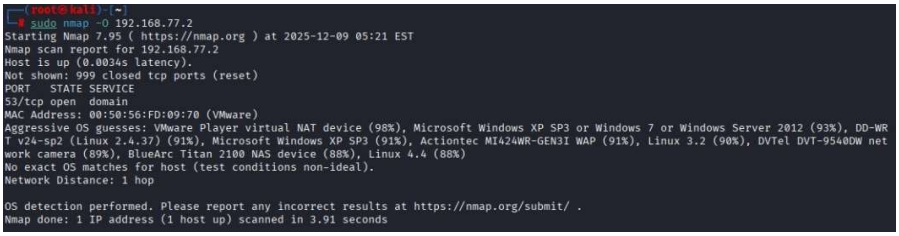
nmap -O 192.168.77.0/24

Tabel 1.6 Hasil Identifikasi Sistem Operasi Target

Hasil	Detail OS	Analisis

OS Terdeteksi	Linux Kernel 3.x – 4.x	Berdasarkan hasil pemindaian pada gambar 1.11, Nmap memprediksi bahwa sistem operasi target berjalan di atas Kernel Linux versi 3.2 – 4.14. Temuan ini sangat kritis karena kernel versi lawas tersebut umumnya diasosiasikan dengan distribusi Linux lama (seperti Ubuntu 14.04 Trusty Tahr). Sistem operasi yang sudah mencapai status *Endof-Life (EOL)* tidak lagi menerima pembaruan keamanan, sehingga sangat rentan terhadap serangan *Kernel Exploit* lokal (misalnya kerentanan *Dirty COW* - CVE-2016-5195) yang memungkinkan penyerang menaikkan hak akses (*Privilege Escalation*) menjadi root."

• Bukti OS fingerprinting



Gambar 1.11 Hasil Identifikasi Sistem Operasi (OS Fingerprinting)

Deteksi kernel Linux versi 3.x - 4.x menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

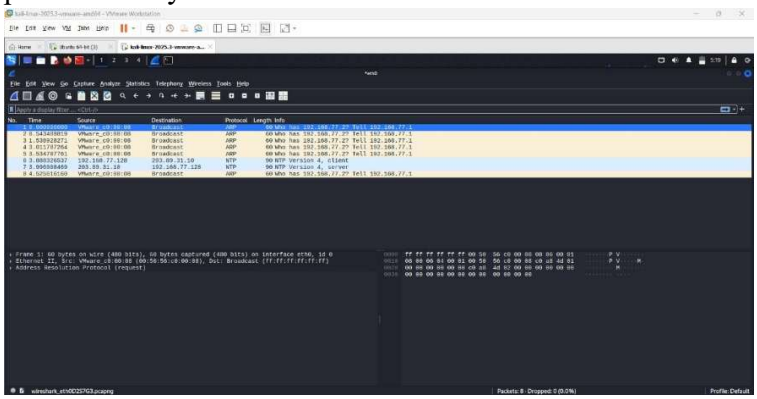
d. Network Protocol Analysis

Tools:Wireshark

Berdasarkan hasil tangkapan trafik pada Gambar 1.12, terlihat jelas anomali pada pola komunikasi *Three-Way Handshake*. Secara normal, koneksi TCP terbentuk melalui urutan SYN → SYN-ACK → ACK. Namun, pada tangkapan ini terlihat urutan:

- Attacker mengirim SYN: Penyerang meminta inisiasi koneksi ke port target.

- Target membalas SYN-ACK: Menandakan bahwa port tersebut dalam status *Open* (terbuka) dan siap menerima koneksi.
- Attacker mengirim RST (Reset): Alih-alih mengirim ACK untuk menyempurnakan koneksi, mesin penyerang justru memutus koneksi secara tiba-tiba.
- Pola ini secara teknis mengonfirmasi penggunaan metode TCP SYN Scan (Stealth Scan) dengan opsi -sS pada Nmap. Teknik ini disebut *'Half-Open Scanning'* karena koneksi tidak pernah benar-benar terbentuk penuh. Tujuannya adalah untuk mendeteksi port terbuka sekaligus menghindari pencatatan (*logging*) pada level aplikasi di server target, yang biasanya hanya mencatat koneksi yang berhasil dibangun sepenuhnya."
- Bukti network protocol analysis



Gambar 1.12 Analisis Paket Jaringan dengan Wireshark

Menangkap pola scanning Nmap, terlihat adanya paket RST yang dikirimkan kembali oleh attacker.

5. KESIMPULAN DAN SARAN a. Kesimpulan

Berdasarkan serangkaian aktivitas *Passive* dan *Active Reconnaissance* yang telah dilakukan, dapat ditarik beberapa kesimpulan penting terkait postur keamanan target:

1. Paparan Informasi Sensitif (Passive Reconnaissance): Pada target *gowakab.go.id*, ditemukan adanya *Information Disclosure* yang signifikan. Teridentifikasinya repositori GitHub publik (dystianen/gowakab) berpotensi memaparkan *source code* atau konfigurasi internal. Selain itu, penemuan struktur organisasi pejabat dan alamat email valid (info@gowakab.go.id) meningkatkan risiko keberhasilan serangan *Social Engineering* dan *Spear Phishing*.

2. Kerentanan Infrastruktur Kritis (Active Reconnaissance): Hasil pemindaian pada target 192.168.77.0/24 menunjukkan tingkat keamanan yang sangat rendah. Ditemukan penggunaan layanan dengan versi yang sudah usang (*outdated*), yaitu OpenSSH 6.6.1p1 dan Apache 2.4.7, serta Sistem Operasi berbasis Kernel Linux lawas (3.x - 4.x) yang telah mencapai status *End-of-Life (EOL)*. Hal ini membuat sistem sangat rentan terhadap eksploitasi CVE publik.
3. Indikasi Backdoor/Malware: Keberadaan Port 6667 dengan layanan IRC (UnrealIRCd/ngircd) pada lingkungan server merupakan anomali besar. Port ini sering diasosiasikan dengan jalur komunikasi *Command and Control* (C2) untuk botnet atau *backdoor* yang ditinggalkan oleh penyerang, menjadikannya prioritas utama untuk investigasi lebih lanjut.
4. Validasi Jaringan: Analisis trafik menggunakan Wireshark berhasil memvalidasi bahwa teknik *Stealth Scan* (SYN Scan) berjalan efektif, terlihat dari pola paket SYN -> SYNACK -> RST. Ini membuktikan bahwa penyerang memiliki visibilitas penuh terhadap jaringan target tanpa terhalang firewall internal yang ketat.

b. Saran dan Rekomendasi

Berdasarkan temuan di atas, berikut adalah rekomendasi perbaikan (remediasi) yang disarankan:

1. Manajemen Aset Digital (Digital Footprint):
   - Segera ubah status repositori GitHub terkait menjadi *Private* atau hapus file sensitif dari riwayat commit.
   - Lakukan pelatihan *Security Awareness* kepada pegawai (khususnya pejabat struktural yang teridentifikasi) mengenai bahaya serangan *Phishing*.
2. Patch Management & Hardening:
   - Lakukan pembaruan (*upgrade*) segera pada Sistem Operasi dan layanan (Apache & OpenSSH) ke versi stabil terbaru untuk menutup celah keamanan (CVE).
   - Nonaktifkan layanan yang tidak diperlukan, terutama Port 6667 (IRC), karena tidak relevan dengan fungsi server web standar.
3. Implementasi Keamanan Jaringan:

- Terapkan *Firewall* (seperti ufw atau iptables) untuk membatasi akses port hanya pada layanan esensial (misalnya hanya port 80/443 dan 22 yang dibuka untuk IP tertentu).
- Gunakan IDS/IPS (*Intrusion Detection System*) untuk mendeteksi pola pemindaian jaringan (seperti SYN Scan) secara *real-time*.